Praxisadresse:

An die
Kassenärztliche Vereinigung

__.__.2020

Widerspruch gegen den Honorarabrechnungsbescheid des Quartals 1/2020

Sehr geehrte Damen und Herren,

in vorbezeichneter Angelegenheit haben wir am ....07.2020 den Honorarabrechnungsbescheid für das oben genannte Quartal erhalten. Gegen diesen legen wir

Widerspruch

ein.

Der Widerspruch erfolgt zunächst zur Fristwahrung.

Uns ist bekannt, dass zu der Frage nach der Rechtmäßigkeit des Honorarabzugs bei Nicht-Anschluss einer Praxis an die sogenannte Telematik-Infrastruktur und Nichtdurchführung des VSDM ein Musterverfahren gegen die KV Baden-Württemberg geführt werden soll.

Das entsprechende Aktenzeichen wird nachgereicht. Gegenstand dieses Verfahrens werden zum überwiegenden Teil die auch uns betreffenden Rechtsfragen sein, sodass wir diesen Widerspruch zur Wahrung unserer Rechte einlegen. Wir beantragen bis zum Abschluss dieses Musterverfahrens das Ruhen dieses Widerspruchverfahrens.

Wir bitten um schriftliche Eingangsbestätigung des Widerspruchs und um Bestätigung der Ruhendstellung dieses Widerspruchverfahrens bis zur Entscheidung der Musterverfahren in Baden-Württemberg.

Begründung:

Die Honorarbescheide für das Abrechnungsquartale I+II +III+IV/2019 und I/2020 sind – soweit es den pauschalen Abzug in Höhe von 1 bzw. 2,5 Prozent des Gesamthonoraranspruchs betrifft – aufzuheben, da die seitens des Gesetzgebers auferlegte Pflicht zur Durchführung des Versichertenstammdatenabgleichs (§ 291 Abs. 2b S. 3 SGB V) mit den derzeit von der gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) zugelassenen Komponenten-Modellen der Telematik-Infrastruktur (TI) für die verpflichteten Leistungserbringer, so also auch für uns als Widerspruchsführer, nur unter Verstoß gegen höherrangiges Recht möglich wäre.

Die Widerspruchsbegründung des I.+II.+III.+IV. Quartals 2019 gilt in vollem Umfang auch als Widerspruch für die KVN Abrechnung des I. Quartals 2020.

In Anlehnung an das Widerspruchsschreiben für die Abrechnung des
IV. Quartals 2019 wird der Widerspruch für das I. Quartal 2020 um einige Punkte ergänzt.

1. Die Realisierung des KVN Citrix VPN erfolgt über eine öffentliche IP, welche derzeit einem Server in Russland zugewiesen ist.

Es klingt schon etwas merkwürdig, dass gerade der DNS- oder Namen Server für das VPN (Citrix) der KVN in Russland liegen soll.
Aber leider ist es so. Das kann man schnell prüfen. Sie loggen sich auf der KVN Webseite ein und rufen in der Dos-Box mit dem Befehl "nsloockup" den

zuständige DNS Server auf.
Dieser hat eine russische IP-Adresse. Ergebnis: IP 188.0.0.1
Wenn man nachschaut, zuwem gehört diese IP Adresse (www.ripe.net), dann erhält man die folgenden Angaben:
Servername: -**srv-gw.rastrnet.ru** - Standort: **Krasnoyarsk, Krasnoyarskiy kray**.

Es handelt sich um eine öffentliche IP-Adresse.

Nur um das richtig zu verstehen, **wenn man** bei einer fehlerhaft aufgebauten VPN-Verbindung (Citrix Client) zur KVN, eine Internet Adresse abfragt, dann bekommt man durch den DNS Server in Russland diese Adresse aufgelöst. Diese von dort erhalte IP Adresse kann nicht das sein, was man wollte.
Und das bedeutet, man hat eine aktive Citrix Client Verbindung mit der KVN, geht auf den eigenen Computer- Bildschirm-Arbeitsplatz zurück und will über"Google" sich zu einem bestimmten Thema schlau fragen. Dann sucht der eig**e**ne Rechner über das bestehende Citrix Client VPN auf dem russischen DNS-Server nach Namensauflösung und wird dorthin gerootet, was der russische Server für die richtige Adresse hält.

Die Brisanz dahinter wird man sofort verstehen, wenn man sich in dieser Situation in guten Glauben bei seiner Bank einloggen möchte.
Weil es eine öffentliche IP ist, landen die Anfragen in ?? Russland.

Weil man sich mit Netz der KVN verbunden hat und parallel eine sensible Adresse aufruft (z.B. www.bank.de), ist es unter den oben genannten

Voraussetzungen durchaus möglich eben nicht mit dem Server der Bank verbunden zu werden.

Damit ist das Sicherheitskonzept der KVN und eventuell der ganzen KBV anzuzweifeln.

Da uns nicht bekannt ist, ob in der TI ähnlich zweifelhafte Konfigurationen vorliegen, halten wird auch das Sicherheitskonzept der TI für zweifelhaft.

Hier verweise ich auf die Aussagen der Gematik GmbH, dass alle Netze in der TI als "sicher" einzustufen wären.

Umso erschreckender finde ist es, dass dieses Desaster offensichtlich bereits seit 2016 bekannt ist. Herausgefunden hatte es damals der Sicherheitsexperte

Chema Alonso. Die Politik wurde 2016 mit Nachdruck auf dieses Desaster hingewiesen. Zum Beleg werden hier nur 2 Quellen angeben:

https://www.allgeier-it.de/security-compliance-loesungen/it-sicherheit-speziell-fuer-medizinische-einrichtungen/
(Kommentare am Ende Pseudonym **rkubbutat**)

https://www.heise.de/ct/artikel/Chema-Alonso-Wir-werden-ein-Riesenproblem-bekommen-3357913.html

Die logische Schlußfolgerung, die man hieraus ziehen muss!
Eine Arztpraxis kann ein so aufgebautes VPN keinesfalls unter Kontrolle bekommen. Soll aber vollumfänglich für eventuelle Sicherheitslecks haften.

2. Sind meine Daten in der Telematik-Infrastruktur (TI) sicher? Oder kann aus einem Teil der TI (VPN Provider) jemand auf meinen Praxisrechner zugreifen?

Die ernstzunehmende Gefahr besteht in jedem Fall durch das neue, vom Konnektor in die TI aufgebaute VPN Netzwerk, welches die Praxis in keiner Weise unter Kontrolle hat. (siehe oben).

<u>Absolute Kurzfassung:</u>
Der Konnektor hat einen TI-VPN Client.
Dieser baut eine Verbindung mittels VPN Provider (Server z.b. bei CGM, DGN, Telekom) in die TI (Bertelsmann) auf.
Der TI-VPN Client (Konnektor) bezieht also seine Routen vom Server (VPN Provider- CGM, DGN, Telekom).

Somit besteht die **Möglichkeit des voll qualifizierten Routings** seitens des VPV-Providers. (= Alleinige Entscheidung des VPN-Providers)

Also Datenpakete aus der Praxis in Richtung TI,
aber eben auch **Datenpakete**, *vom VPN-Provider gestattet* (geroutet),
aus der TI in die Praxis.

Damit erhält der VPN-Provider (Server z.b. bei CGM, DGN, Telekom) und damit die TI (Bertelsmann) potentiell Zugriff auf auf das gesamte Praxisnetzwerk jeder einzelnen Arztpraxis, weil der Konnektor ein Teil dieses, vom Praxisinhaber nicht verhinderbaren "TI-Netzwerkes", ist.

Im Szenario - Konnektor im Reihenbetrieb -
ist der Konnektor das Standard Gateway. Also absolut alle Datenpakete gehen über den Konnektor. *(Datenschutz-Supergau)*

Im Szenario - Konnektor im Parallel Betrieb -
ist der Zugriff auf das Praxisnetzwerk nicht ganz so einfach wie im Reihenbetrieb, weil der Konnektor nicht unbedingt das Standard Gateway ist.

Die Einflussnahme der Praxis auf die Sicherheit des Routing's ist gleich NULL!!!

Es sei denn, man sperrt den Konnektor (VPN Client) aus dem Netzwerk aus.

Grundlagen Netzwerk:
Ein Client (egal ob Windows, Linux, MacOS oder . . .) sendet seine Daten zum Ziel mit folgender Methode.

Beispiel:
Das Netzwerk des Client sei 192.168.121.0/24 (also 255 Clients 192.168.121.0 bis 192.168.121.254)
Das Standard Gateway sei 192.168.121.199

Anhand der Subnetzmaske (/24) erkennt der Client wohin er das Datenpaket senden muss. Jedes Datenpaket im eigenen Netzwerk (192.168.121.0/24) kann er direkt zustellen.

Jedes Datenpakt in andere Netze sendet er zum Standard Gateway (eventuell Konnektor [Reihenbetrieb]).
Dieser wiederum kennt seine Netze und die dazugehörigen Standard Gateway's und er verfährt mit den Datenpakete ebenso.

Hier gibt es Schnittpunkte zum ersten Abschnitt in diesem Schreiben, man erinnert sich an die öffentliche, russische IP 188.0.0.1 .
Jeder Knoten, welcher die Daten weiter transportiert, kann auch **in** die Daten schauen!
Damit das nicht so einfach geht werden diese verschlüsselt.
Dabei kann der Sender der Daten seine eigenen Daten nicht entschlüsseln, da er nicht im Besitz des privaten Schlüssels ist.
Der Konnektor hat dazu 2 öffentliche Schlüssel im Zugriff.
Die SMC-KT und die SMC-B Karte.

Mit der SMC-B Karte (Schlüssel) werden die Patientendaten verschlüsselt.
Mit der SMC-KT Karte (Schlüssel) wird das bereits verschlüsselte Patienten Datenpaket für den Transport durch das Internet verschlüsselt.
Der VPN Provider hat hierfür den Privaten Schlüssel (SMC-KT).

Die komplette Sicherheit der ganzen TI liegt in den Händen der VPN-Provider!!

Die komplette Datenspeicherung der Gesundheitsdaten von ca. 73 Millionen Menschen liegt in der Hand einer privaten Firma!!
Das darf nicht sein. Es gibt genügend Gründe, dass diese Daten unrechtmäßig geklont und mißbraucht werden könnten.

Erinnerung:
Wiederholung aus Widerspruch zur KVN Abrechnung 4. Quartal 2019:
In dem **Schutzprofil BSI-CC-PP-0047-2015** finden sich entgegen § 291b Abs. 1 S. 4 SGB V keine technischen Anforderungen zum Schutz der Patientendaten im IT-System der Arztpraxis. Das Schutzprofil adressiert ausschließlich den Schutz der Telematikinfrastruktur und des dortigen Datenverkehrs von außen, nicht aber den Schutz des Datenbestands in der Arztpraxis gegen IT Angriffe aus bzw. über die Telematik-Infrastruktur,
obwohl der Schutz der in der Arztpraxis gespeicherten Patientendaten (Befunde, Krankheitsgeschichten etc.) wesentlich wichtiger ist als die bloßen Versichertenstammdaten.

Ebenfalls sollten, auf Anweisung der GEMATIK GmbH die VPN-Provider durch das BSI nicht geprüft werden und gelten durch Ihre "Geburt" als vertrauenswürdig.

Weiteres Datenschutzproblem:
Die so transportierten Daten bestehen auch aus **Metadaten** (s.o. Datenpaket Aufbau) , welche auf dem Weg vor dem eigentlichem Ziel entschlüsselt werden.
Hier dürfte mindestens der Datenschutz des VPN - Provider´s gegenüber dem Leistungserbringer zweifelhaft sein.

Problem Datenschutz und Haftung:
Laut offizieller Lesart haften die niedergelassenen Ärztinnen und Ärzte für die Patienten-Daten bis zum Konnektor.

Bei normalem Schutz der Praxis durch eine zentrale Firewall könnten Patienten-daten nur über diese auch abfließen.

Da nun aber 2 mögliche Internetverbindungen (Konnektor + eigene Internet-Verbindung) in einer Arztpraxis in Betracht kommen, kann ein Leistungserbringer nicht verhindern oder beweisen, dass Patienten-Daten über den Konnektor abgeflossen sind (keinerlei Einflussnahme). Es sei denn, der Konnektor ist nicht im Praxisnetzwerksegment integriert.

Bei dem aktuellen Aufbau der TI mit den Konnektoren in den Praxisnetzen ist es zu keinem Zeitpunkt beweisbar, über welche der Verbindungen Daten aus der jeweiligen Arztpraxis abgeflossen sind.

Das entspricht nicht den gegenwärtigen Vorschriften der Datenschutzgrundverordnung (DSGVO).

Es fehlt weiterhin eine offizielle Datenschutzfolgeabschätzung der Gematik als Betreiber der TI. Solange diese nicht vorliegt, dürften keinerlei Daten in die TI eingespielt oder auch keine Praxis den Konnektor an die TI anschließen. Denn keiner gibt dafür Gewähr, dass nicht aus der TI selbst über das bestehende VPN Angriffe auf die Praxis erfolgen. Denn das ist prinzipiell möglich.

Zudem führen diese Datenschutzverstöße sowie die konkret nachweisbaren Sicherheitsmängel der Telematik-Infrastruktur im Ergebnis zu einem von uns nicht hinzunehmenden, unverhältnismäßigen Eingriff in unsere Berufsausübungsfreiheit gemäß Art. 12 GG.

Der derzeitige Zustand führt bei den Ärzten und Psychologischen Psychotherapeuten zu einem datenschutzrechtlich rechtswidrigen Zustand und zu erheblichen Gefährdungen der auf der elektronischen Gesundheitskarte gespeicherten Patientendaten und der im Praxisinformationssystem der Praxis gespeicherten weiteren Gesundheitsdaten.

Problem der Datenverfügbarkeit und fehlenden Plan B:

in den zurückliegenden Wochen haben wir es durch eine mehrwöchige Störung der TI erfahren, wie verletzlich dieses System ist. Der Ausfall der Konnektoren bei ca. 80.000 Ärztinnen und Ärzten führte gleichtzeitig auch zu einem Vertrauensverlust in das TI - System auf breiter Basis. Den Grund dafür kann man gut in dem Heise Artikel unter dem folgenden Link nachlesen:

https://www.heise.de/news/Analyse-Warum-80.000-Arztpraxen-ihre-Verbindung-zur-Telematik-verloren-4842866.html

Der angegriffene Honorarbescheid ist demnach insoweit aufzuheben.

3. Musterverfahren in Baden-Württemberg

Wie wir Ihnen bereits mitteilten, läuft demnächst in dieser Angelegenheit in Baden-Württemberg ein Musterverfahren. Das entsprechende Aktenzeichen wird nachgereicht. Gegenstand dieses Musterverfahrens werden zum überwiegenden Teil die auch uns betreffenden Rechtsfragen sein, sodass dieser Widerspruch (auch) zur Wahrung unserer Rechte eingelegt wird.

Wir beantragen daher nochmals, das streitgegenständliche Widerspruchs-verfahren bis zum rechtskräftigen Abschluss des Musterverfahrens ruhend zu stellen. Dies nicht zuletzt um eine KV-übergreifende, einheitliche und rechtssichere Entscheidung in dieser Sache zu treffen.

Nach weiteren Informationen zur Sicherheit der einzelnen Komponenten, Kartenlesegerät, Konnektor, Heilberufsausweis und Patientenkarte (sGK), auf dem Jahreskongress des Chaos Computer Clubs in Hamburg Ende Dezember 2019, sowie zur Sicherheit der benutzten Software in den Konnektoren lt. eines Berichtes der Computerzeitschrift c´t im Januar 2020 (Quelle: https://www.heise.de/select/ct/2020/3/1580498856872446), erlauben wir uns diesen Widerspruch jederzeit noch zu ergänzen und hoffen auf Ihr Verständnis.

Wir danken Ihnen für Ihre Geduld und bitten um schriftliche Eingangsbestätigung der Widerspruchsbegründung und um Bestätigung der Ruhendstellung dieses Widerspruchverfahrens bis zur rechtskräftigen Entscheidung der Musterverfahren in Baden-Württemberg.

Mit freundlichen Grüßen

.....

Unterschrift und Stempel